2.2.4 Notfallorganisation und 4.0-Prozesse

Stichwörter: Angriffe, IT-Sicherheit, kritische Situationen, Notfälle, Notfallmanagement, Notfallvorsorgekonzept, Schadensanalyse, Sicherheitsorganisation, Zwischenfälle

› Warum ist das Thema wichtig?

Der Einsatz von intelligenter Software[1] mit Modellen der künstlichen Intelligenz (KI) stellt neue Anforderungen an die Notfallorganisation von Unternehmen. Die Komplexität sowie die technische Autonomie der cyber-physischen Systeme (CPS)[2] mit ihrer 4.0-Technologie[3] können zu einer Vielzahl von neuen Schadensereignissen im Betrieb führen. Gleichzeitig ergeben sich neue Möglichkeiten für die Notfallorganisation in Unternehmen, weil mehr Informationen beinahe in Echtzeit zur Verfügung stehen und ein zeitlich und örtlich flexibler Zugriff möglich ist. Aufgrund der zunehmenden Vernetzung der 4.0-Prozesse[4] sowohl betriebsintern als auch -extern nimmt die Bedeutung einer systemischen und prozessorientierten Sicht auf die Notfallorganisation zu: Einzelne Schadensereignisse können eine immer größere Bedeutung für das gesamte Unternehmen sowie für seine Akteure gewinnen.

› Worum geht es bei dem Thema?

Begriffe: Notfallorganisation – Sicherheitsorganisation – Notfallmanagement

Die **Notfallorganisation** umfasst die Festlegung betrieblicher Maßnahmen, um Schäden nach Schadensereignissen (Zwischenfälle, Notfälle und andere kritische Situationen) von Menschen, dem Betrieb oder der Umwelt so gering wie möglich zu halten. Die Notfallorganisation soll zudem sicherstellen, dass wichtige Geschäftsprozesse selbst in kritischen Situationen nicht oder nur temporär unterbrochen werden und die wirtschaftliche Existenz der Institution auch bei einem größeren Schadensereignis gesichert bleibt. [5]

Die **Sicherheitsorganisation** umfasst alle strukturellen und prozessorientierten Maßnahmen des Unternehmens in den Bereichen

- IT-Sicherheit und Security sowie
- Sicherheit und Gesundheit bei der Arbeit (Safety).

Ziel der Notfall- und Sicherheitsorganisation ist es, präventiv Schadensereignisse (Zwischenfälle, Notfälle und andere kritische Situationen) zu verhindern.[6] Ziel der Arbeitsorganisation und Unternehmenskultur ist es, präventiv produktive, sichere und gesundheitsgerechte Arbeitsabläufe zu ermöglichen.[7]

Unter **Notfallmanagement** sind die Prozesse, Verhaltensweisen und koordinierten Tätigkeiten zu verstehen, die eine Organisationseinheit ausführen muss, um drohende Notfälle zu verhindern oder bereits eingetretene zu bewältigen.

Mögliche Ursachen für Schadensereignisse beim Einsatz von 4.0-Technologien

Zwischenfälle, Notfälle und andere kritische Situationen können beim Einsatz von 4.0-Technologien folgende Ursachen haben – *siehe Abbildung 1:*

- Ungenügende IT-Sicherheit und Datensicherheit – zum Beispiel durch Schadprogramme („Viren“), Angriffe Dritter (Hacker), ungenügend gesicherte Plattformen und Clouds, Stromausfall › *siehe Umsetzungshilfen 2.2.3 Risikobetrachtung und IT-Sicherheit; 2.3.1 Datensicherheit in 4.0-Prozessen; 2.5.1 Anforderungen an eine Cloud; 2.5.3 Plattformökonomie*.
- Natur- und Betriebsereignisse, die Schäden an 4.0-Technologien verursachen – zum Beispiel durch Brände, Wassereinbruch, Hochwasser, Unwetter, Sturm
- Mängel bei Planung- und Organisation des Einsatzes der 4.0-Technologie – zum Beispiel durch ungenügende Datenqualität, unzureichenden Datenschutz, falschen Umgang und unberechtigten Zugriff durch Beschäftigte und vernetzte Akteure, mangelhafte Risikobetrachtung und Gefährdungsbeurteilung, fehlende Qualifizierung, fehlende Anweisungen und Vereinbarungen im Umgang mit den 4.0-Technologien › *siehe Umsetzungshilfen 1.4.2 Kompetenzen im Führungspro-*

Diese Umsetzungshilfe gibt Experten und Interessierten Anregungen, wie Arbeit 4.0 zu gestalten ist. Die Empfehlungen sollten an die jeweilige konkrete betriebliche Situation angepasst werden.

[1] Intelligente Software steuert cyber-physische Systeme (CPS) und andere autonome technische Systeme (wie Messenger-Programme). Intelligente Software nutzt Modelle künstlicher Intelligenz zusammen mit anderen Basistechnologien wie zum Beispiel Algorithmen, semantischen Technologien, Data-Mining. Intelligente Software ist autonom und selbstlernend.

[2] Cyber-physische Systeme (CPS) verbinden und steuern als autonome technische Systeme Arbeitsmittel, Produkte, Räume, Prozesse und Menschen beinahe in Echtzeit. Die komplette oder teilweise Steuerung übernimmt die intelligente Software auf Grundlage von Modellen der künstlichen Intelligenz. Genutzt werden dazu unter anderem auch Sensoren/Aktoren, Verwaltungsschalen, Plattformen/Clouds.

[3] 4.0-Technologie bezeichnet hier Hardware und technologische Produkte (wie Assistenzmittel/Smartphones, Sensoren/Aktoren in smarten Arbeitsmitteln, Fahrzeugen, Produkten, Räumen usw., smarte Dienstleistungen, Apps), die von intelligenter Software (inkl. KI) ganz oder teilweise gesteuert werden.

[4] Unter 4.0-Prozessen werden hier alle Arbeitsprozesse verstanden, in denen cyber-physische Systeme (CPS) oder andere autonome technische Systeme (wie Plattformen, Messenger-Programme) beteiligt sind. 4.0-Prozesse sind in den Arbeitsprozessen bisher selten vollständig, aber in Ansätzen in allen Betrieben umgesetzt.

[5] BSI-Standard 100-4, S. 1; VBG 2017, S. 38

[6] VBG 2017, S. 39

[7] VBG 2017, S. 38

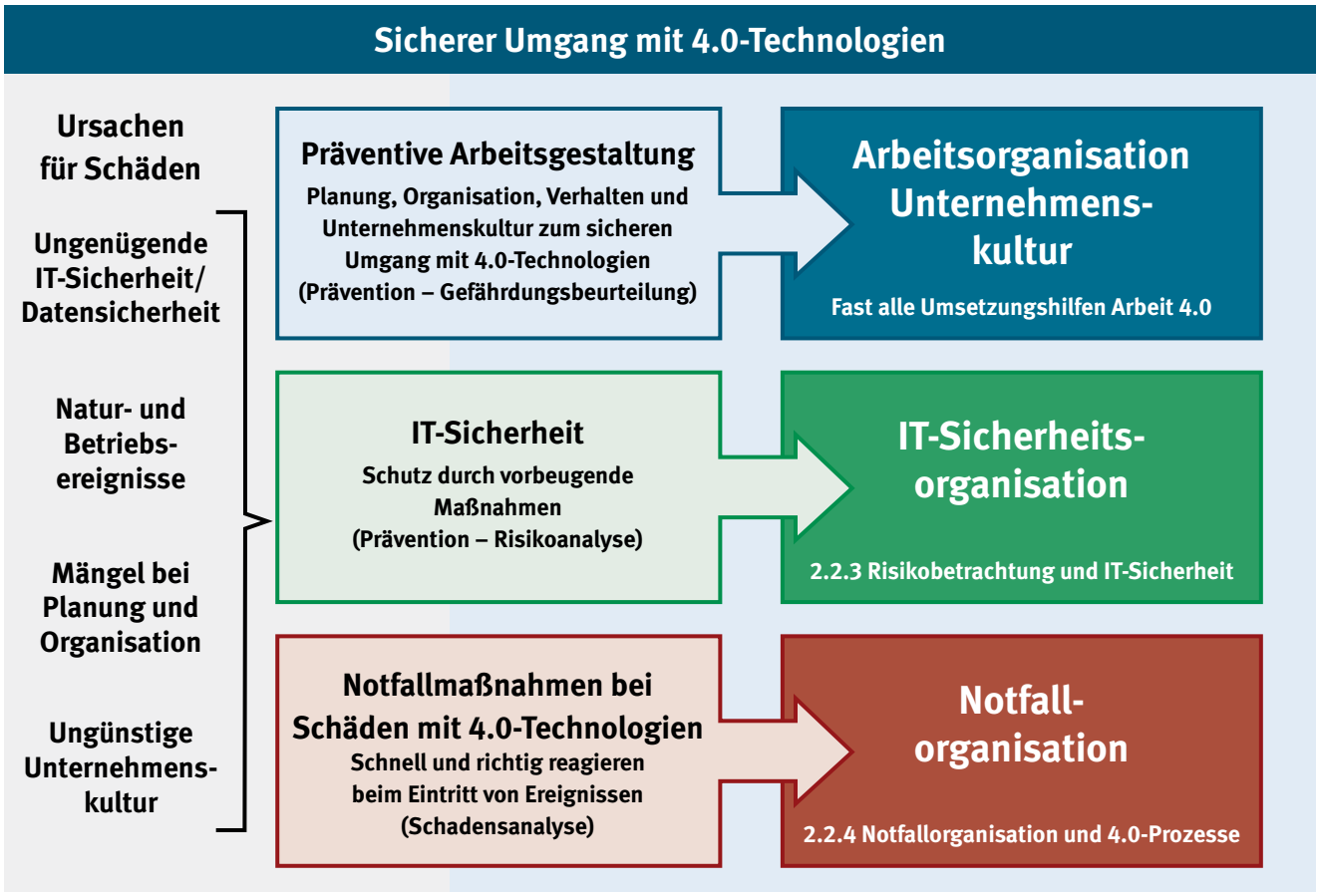

Abbildung 1: Notfall- und Sicherheitsorganisation beim Umgang mit 4.0-Technologien (eigene Darstellung)

zess 4.0; 1.4.3 Kompetenzen der Beschäftigten in 4.0-Prozessen; 2.1.2 Integration von intelligenter Software (inkl. KI) in die Organisation; 2.2.2 Gefährdungsbeurteilung 4.0; 2.4.1 Prozessplanung mit CPS.

- Eine Unternehmenskultur, die das Bewusstsein im sicheren Umgang mit Daten nicht fördert – zum Beispiel durch fehlende Kriterien und Werte im Umgang mit 4.0-Technologien, fehlende Kenntnisse und Kompetenzen, fehlende Motivation und Bereitschaft, Mängel in der Führung, keine Fehlerkultur, ungenügende Einbindung und Beteiligung der Führungskräfte und Beschäftigten › *siehe Umsetzungshilfen 1.1.5 Kriterien zur Erklärbarkeit der 4.0-Technologien; 1.2.1 Führung und 4.0-Prozesse; 1.4.2 Kompetenzen im Führungsprozess 4.0; 1.4.3 Kompetenzen der Beschäftigten in 4.0-Prozessen; 1.5.1 Unternehmenskultur in 4.0-Prozessen*.

Diese Faktoren können durch und auf die 4.0-Technologien und die intelligente Software (inkl. KI) wirken und im Betrieb beispielsweise zu folgenden Bedrohungen und Schäden führen:

- Bei Personen im Betrieb: Zum Beispiel kann intelligente Software (inkl. KI) Arbeitsmittel fehlsteuern. Hierdurch kann es zu Kollisionen oder unkontrollierten Bewegungen und Abläufen kommen. In der Kollaboration von Personen mit Assistenzsystemen (zum Beispiel Exoskelette, Roboter, Virtual Reality) können Menschen direkt mit der Technik verbunden sein, sodass Störungen und Ausfälle der Software Beschäftigte schädigen können. Auch personenbezogene Daten von Führungskräften und Beschäftigten können missbraucht werden. › *Siehe Umsetzungshilfen 2.3.2 Datenschutz in 4.0-Prozessen; 3.2.4 Exoskelette; 3.2.6 Augmented Reality – Virtual Reality; 3.2.7 Nutzung von Robotern*.
- In der Infrastruktur: Zum Beispiel kann die Organisationssoftware (inkl. KI) durch unberechtigte Fremdzugriffe/ Sabotage, Datenmanipulation und Datendiebstahl geschädigt werden und es kann zu Störungen der Arbeitsabläufe kommen. Naturereignisse (zum Beispiel Feuer, Wasser, klimatische Bedingungen) und Brände können die Funktionsweise der intelligenten Software (inkl. KI) beeinträchtigen oder sie ausschalten. Möglich sind auch der Ausfall und die Beeinträchtigung von smarten Gebäudetechnologien durch Manipulation, was zum Beispiel den Zutritt zu Gebäuden verhindern kann.
- Eigenständige Entscheidungen der intelligenten Software (inkl. KI): Zum Beispiel kann die intelligente Software (inkl. KI) durch Fehlsteuerungen oder Schadprogramme geschädigt werden und Situationen herbeiführen, auf die die Beschäftigten nicht vorbereitet sind. Die Beschäftigten müssen auf diese unerwartet auftretenden Störungen akut reagieren, sodass dies zu Störungen im Ablauf, Unfällen oder Behinderungen führen kann.
- Bei Dritten (wie Kunden, Dienstleistern, Partnern): Zum Beispiel kann durch Datenmissbrauch oder Fehlsteuerung von Prozessen (zum Beispiel Produktionsanlagen, Lagerhaltung) intelligente Software (inkl. KI) in der Funktionsweise beeinträchtigt

werden, die mit Netzen anderer Unternehmen verbunden sind. Dadurch können Dritte gefährdet werden. Es kann Misstrauen bei Kunden, Partnern und Dienstleistern entstehen oder das Image des Betriebes kann geschädigt werden.

Notfallorganisation zu Schadensereignissen durch 4.0-Technologien

Während bei der Nutzung von 4.0-Technologien die IT-Sicherheit generell ein wichtiges Thema ist, sollten sich Betriebe auch auf Zwischenfälle, Notfälle und andere kritische Situationen durch 4.0-Technologien vorbereiten. Für kleine und mittlere Unternehmen ist ein umfassendes Notfallmanagement – zum Beispiel nach BSI-Standard 100-4 – oft nicht umsetzbar. Trotzdem sollten auch kleine und mittlere Unternehmen in Anlehnung an die Standards für große Betriebe einige Maßnahmen der Notfallorganisation beim Einsatz der 4.0-Technologien planen und umsetzen. Wenn jede Führungskraft und jeder Beschäftigte sofort weiß, was bei Zwischenfällen, Notfällen und anderen kritischen Situationen durch 4.0-Technologien zu tun ist, können die Auswirkungen des Schadens begrenzt werden.

Im Folgenden sind einige grundlegende Hinweise zur Notfallorganisation im Umgang mit 4.0-Technologien zusammengefasst. Die hier skizzierten Hinweise bauen auf einer funktionierende IT-Sicherheit auf › *siehe Umsetzungshilfe 2.2.3 Risikobetrachtung und IT-Sicherheit*.

Notfallorganisation und IT-Sicherheit sollten zusammen betrachtet werden. Das bedeutet, dass die *Leitung des Unternehmens auch die Verantwortung für die Notfallorganisation* beim Umgang mit 4.0-Technologien haben sollte.[8] Sie sollte auch die Grundlagen für die Notfallorganisation (Notfallstrategie) festlegen. Hierzu können folgende Punkte zur Orientierung dienen:

- Diejenigen Geschäftsziele definieren, die durch Schäden im Umgang mit 4.0-Technologien gefährdet werden könnten.
- Die Schäden durch die verwendeten 4.0-Technologien beschreiben, die besonders schwerwiegende Auswirkungen haben könnten.
- Die Unterbrechungen der Arbeitsprozesse durch Schäden der verwendeten 4.0-Technologien beschreiben, die als existenzbedrohend angesehen werden.
- Festlegen, welche Schäden eher akzeptiert werden können und welche nicht.

Für die ermittelten kritischen Prozesse und Ressourcen sollten eine *Schadensanalyse*[9] und eine Risikoanalyse › *siehe Umsetzungshilfen 2.2.1 Risikobetrachtung von 4.0-Prozessen; 2.2.3 Risikobetrachtung und IT-Sicherheit* durchgeführt werden (wie zum Beispiel Beeinträchtigung der Aufgabenerfüllung, finanzielle Auswirkung, negative Innen- und Außenwirkung, Verstoß gegen Gesetze). Dabei sollte die Frage geklärt werden: „Wodurch werden meine Prozesse und Ressourcen bedroht?“ Sind diese Aspekte bereits in der Risikobetrachtung zur IT-Sicherheit erhoben und beantwortet, kann auf diese Ergebnisse zurückgegriffen werden.

Für die Notfallorganisation bei Schadensereignissen durch 4.0-Technologien sollte *die Verantwortung einer Führungskraft übertragen* werden. In kleinen und mittleren Unternehmen ist es sinnvoll, dass dies dieselbe Person ist, die auch für die IT-Sicherheit verantwortlich ist. Diese verantwortliche Führungskraft sollte – wie auch bei der IT-Sicherheitskonzeption – bei der Notfallorganisation einen unabhängigen IT-Experten hinzuziehen. Außerdem ist es sinnvoll, ein Budget für die Notfallorganisation festzulegen.[10]

Die verantwortliche Person für die Notfallorganisation sollte ein *Konzept und eine Verhaltensanweisung (eine Leitlinie/ ein Notfallvorsorgekonzept)* erstellen.[11] Diese Anweisung könnte unter anderem folgende Inhalte haben[12]:

- Ziel und Stellenwert der Notfallorganisation
- Geltungsbereich (wie zum Beispiel Betriebsstätten, Arbeitsplätze, Arbeitsabläufe, Projekte)
- Verantwortliche Person und weisungsbefugten Personen
- Mögliche Bedrohungen durch die verwendeten 4.0-Technologien
- Mögliche Auswirkungen auf 4.0-Technologien
- Maßnahmen, die beim Eintreten des Schadensfalls zu ergreifen sind und die ein schnelles und sinnvolles Reagieren auf einen Vorfall ermöglichen
- Wichtige Zuständigkeiten bei den Maßnahmen der Notfallorganisation
- Festgelegten Vorsorgemaßnahmen, wie beispielsweise die Meldetechnik (auch für vernetzte Plattformen anderer Unternehmen), Ausweichstandorte, Alarmierungsverfahren, Datensicherung oder im Notfall relevante Vereinbarungen mit externen Dienstleistern
- Integration der Notfallorganisation in alle relevanten Geschäftsprozesse beziehungsweise Verfahren und Projekte
- Regelmäßige Überprüfungen, Tests und Übungen; die relevanten Gesetze, Richtlinien und Vorschriften, die zu beachten sind
- Verfahren des Verbesserungsprozesses der Notfallorganisation, Pflege und Überarbeitung der Notfallorganisation

Diese *Anweisung* (Leitlinie, Notfallvorsorgekonzept) der Notfallorganisation bei Schadensereignissen durch 4.0-Technologien sollte *allen Führungskräften und Beschäftigten zur Verfügung* stehen und im Betrieb aushängen. Außerdem ist sie allen Führungskräften und Beschäftigten zum Beispiel in Teambesprechungen bekannt zu machen. Maßnahmen zur Notfallorganisation und zu Schadensereignissen durch 4.0-Technologien sollten zum Bestandteil des Alltagshandelns der Führungskräfte und Beschäftigten werden (zum Beispiel durch *regelmäßige Sensibilisierungsmaßnahmen* wie Teambesprechungen, themenbezogene Veranstaltungen, Schulungen oder Übungen). Dies ist ein wesentlicher Bestandteil des Verbesserungsprozesses und trägt gleichzeitig zur Sensibilisierung im Umgang mit den Maßnahmen bei.

Hilfreich ist es auch, die Konzepte und Verhaltensanweisungen der Notfallorganisation zu *dokumentieren*, um getroffene Entscheidungen nachvollziehen zu können, Handlungen wiederholbar zu machen sowie Abläufe und Maßnahmen nachweisen zu können[13] – auch wenn diese Dokumentation vor allem für kleine Betriebe immer einen hohen Aufwand bedeutet.

[8] BSI-Standard 100-4, S. 15ff.
[9] Business Impact Analyse, BSI-Standard 100-4, S. 29
[10] BSI-Standard 100-4, S. 62
[11] BSI-Standard 100-4, S. 30ff.
[12] BSI-Standard 100-4, S. 59f.
[13] BSI-Standard 100-4, S. 11

4.0-Technologien für die Notfallorganisation nutzen

4.0-Technologien können die Notfallorganisation im Betrieb auch unterstützen. Sie können vor allem in der Ablauforganisation der Notfälle wichtige Hilfen bieten. Beispiele dazu sind der Tabelle 1 zu entnehmen.

Für die Umsetzung der Notfallorganisation gibt es mittlerweile Softwaretools. Kriterien für die Auswahl dieser Tools finden sich im BSI-Standard 100-4 ab Seite 98ff.

Aspekte der Notfallplanung in Anlehnung an DIN EN ISO 45001:2018-06 | **Tabelle 1**

Aspekte der Notfallorganisation (Ablauforganisation) – Beispiele	Unterstützung durch 4.0-Technologien – Beispiele
Ermittlung von möglichen Notfallsituationen	Einsatz von Virtual Reality (VR) und Simulation von Ereignissen
Möglichkeiten des (frühzeitigen) Erkennens von Notfallsituationen und der Ermittlung des Schadensausmaßes	Sensortechnologie und Echtzeitkommunikation, frühzeitiges automatisches Gegensteuern durch intelligente Software (inkl. KI)
Festlegung einer geplanten Reaktion auf Notfallsituationen einschließlich der Versorgung durch Erste Hilfe	Einsatz von 4.0-Technologien bei der Reaktion auf Ereignisse, zum Beispiel autonomes Abschalten von Anlagen in Notfallsituationen
Schulungen über das Verhalten bei Notfallmaßnahmen	Individualisiertes E-Learning und Lernen im simulierten Umfeld (VR)
Wiederkehrende Überprüfung und Übung des geplanten Verhaltens in Notfällen	Unterstützung der Überprüfung zum Beispiel durch Auswertung des Verhaltens durch intelligente Software (inkl. KI) und Bereitstellung relevanter, priorisierter Informationen beinahe in Echtzeit
Befall der 4.0-Technologie von Anlagen, Komponenten und Meldesystemen durch Schadprogramme	Selbstüberwachung der 4.0-Technologie von Anlagen, Komponenten und Meldesystemen gegen Schadprogramme
Kommunikation in Notfallsituationen	Individualisierte Informationen durch intelligente Software (inkl. KI); Verkürzung von Kommunikationszeiten durch 4.0-Technologien
Überprüfung des Verhaltens nach dem Eintritt von Notfallsituationen	Bewertung des Verhaltens durch intelligente Software (inkl. KI)
Kommunikation und Bereitstellung relevanter Informationen an alle Beschäftigten bezüglich ihrer Pflichten und Verantwortlichkeiten in Notfällen	Nutzung von Smart Devices (zum Beispiel Smartphones) zur Bereitstellung von Informationen beinahe in Echtzeit; Auswahl durch intelligente Software (inkl. KI), welche Informationen an wen auf welches Endgerät gesendet werden
Kommunikation relevanter Informationen an Auftragnehmer, Notfalldienste, Behörden und Gemeinden sowie weitere interessierte Gruppen	Informationen beinahe in Echtzeit, Auswahl durch intelligente Software (inkl. KI), welche Informationen an wen gesendet werden
Kommunikation innerhalb der betriebsinternen Notfallorganisation	Informationen beinahe in Echtzeit, virtuelle Konferenzen und Treffen
Alarmierung, Information im Notfall und Evakuierung von Beschäftigten und Gästen des Hauses	Unterstützung durch smarte Endgeräte (zum Beispiel Smartphones)

Welche Chancen und Gefahren gibt es?

Ist die Notfallorganisation für den Umgang mit 4.0-Technologien genügend beziehungsweise ungenügend gestaltet, kann dies unter anderem folgende positive beziehungsweise negative Auswirkungen haben:

Chancen – Beispiele	Gefahren – Beispiele
Frühzeitiges Erkennen von Zwischenfällen, Notfällen und anderen kritischen Situationen und damit frühzeitige Reaktion	Zu spätes Erkennen von Zwischenfällen, Notfällen und anderen kritischen Situationen und damit unzureichende Reaktion
Geordnete und abgestimmte Reaktionen auf Zwischenfälle, Notfälle und andere kritische Situationen durch 4.0-Technologien mit geringeren Überraschungseffekten, da Führungskräfte und Beschäftigte für schnelle Reaktionen im Notfall befähigt sind	Unzureichend abgestimmte Reaktionen auf Zwischenfälle, Notfälle und andere kritische Situationen durch 4.0-Technologien mit hohen Überraschungseffekten, da Führungskräfte und Beschäftigte keine Kompetenzen besitzen, wie sie sich im Notfall verhalten sollen
Geringere Auswirkungen auf Arbeitsprozesse durch Störungen aufgrund von 4.0-Technologien durch systematische und rechtzeitige Reaktion auf Schadensfälle – weniger Schäden und Ausfallstunden, kürzere Wiederanlaufzeiten	Negative Auswirkungen auf Arbeitsprozesse durch Störungen aufgrund von 4.0-Technologien durch fehlende Reaktion auf Schadensfälle mit hohen Schäden und Ausfallstunden sowie langen Wiederanlaufzeiten
Direkte und gezielte Informationen an vernetzte Akteure (wie Plattformen, andere Unternehmen, Kunden, Dienstleister) bei Störungen aufgrund von 4.0-Technologien	Fehlerhafte Informationen an vernetzte Akteure (wie Plattformen, andere Unternehmen, Kunden, Dienstleister) mit kritischen Folgesituationen und Haftungsproblemen
Kostenersparnis durch optimale Reaktion auf Zwischenfälle, Notfälle und andere kritische Situationen durch 4.0-Technologien und Eindämmung der Schadensfolgen	Hohe Kosten durch verspätete und unstrukturierte Reaktion auf Zwischenfälle, Notfälle und andere kritische Situationen durch 4.0-Technologien mit hohen Schadensfolgen

Wer 4.0-Technologien für die Notfallorganisation einsetzt, hat unter anderem folgenden Nutzen beziehungsweise folgende Nachteile:

Chancen – Beispiele	Gefahren – Beispiele
Frühzeitige Analyse und frühzeitiges Erkennen von kritischen Zuständen und Situationen	Kritische Zustände und Situationen werden nicht oder zu spät erkannt
Information durch intelligente Software (inkl. KI) über kritische Zustände und Situationen beinahe in Echtzeit	Fehlende Informationen über kritische Zustände und Situationen
Individuelle Anweisungen in Notfällen bei Schadensereignissen	Keine individuellen Anweisungen in Notfällen bei Schadensereignissen
Simulation von Notfallszenarien durch Virtual Reality (VR) für Trainings	Fehlende Sensibilisierungsmöglichkeiten bei Notfallsituationen
Autonome Abwehr von Schadprogrammen und Hackerangriffen	Unzureichende Abwehr von Schadprogrammen und Hackerangriffen

Welche Maßnahmen sind zu empfehlen?

Für eine systematische Notfallorganisation unter Berücksichtigung der 4.0-Technologien sind unter anderem folgende Maßnahmen zu empfehlen:

- Die Unternehmensleitung sollte festlegen, welche grundlegenden Ziele die Notfallorganisation haben soll und welche Geschäftsprozesse und Abläufe besonders geschützt werden sollen.
- Benennung einer verantwortlichen Führungskraft für die Notfallorganisation (kann dieselbe Person sein, die auch für die IT-Sicherheit und die Sicherheitsorganisation verantwortlich ist). Auch festlegen, welcher unabhängige IT-Experte den Verantwortlichen unterstützt und berät.

- Analysieren, welche Notfälle durch 4.0-Technologien sowie interne und externe Vernetzung möglich sind, welche Auswirkungen diese haben können und wer betroffen sein kann.
- Arbeitsanweisung (Leitlinie/Notfallvorsorgekonzept) erstellen, die die Verfahren und Maßnahmen der Notfallorganisation bei Schäden durch 4.0-Technologien festlegt.
- Unterweisungen, Schulungen und Tests zu 4.0-Notfällen festlegen, insbesondere deren Auswirkungen, Erkennbarkeit und Regelungen für Meldungen und Verhaltensmaßnahmen in Notfällen.
- Nutzung von Simulationen (zum Beispiel Virtual Reality) zur Erarbeitung von Störungsszenarien und zum Üben, wie mit Störungen umzugehen ist.
- Regelmäßig die Wirksamkeit der Notfallorganisation mit Führungskräften und Beschäftigten in Teamtreffen diskutieren sowie Verbesserungsmaßnahmen besprechen.

Die Führungskräfte sollten sich informieren und beraten lassen, wie die 4.0-Technologie für die Notfallorganisation zu nutzen ist und welche Anwendungen für ihre Branche angeboten werden.

Quellen und weitere Informationsmöglichkeiten:

BSI-Standard 100-4: *Notfallmanagement Version 1.0*.

DIN ISO 45001:2018-06. *Managementsysteme für Sicherheit und Gesundheit bei der Arbeit – Anforderungen mit Anleitung zur Anwendung*. Beuth-Verlag.

VBG (2017). *Zwischenfall, Notfall, Katastrophe. Leitfaden für die Sicherheits- und Notfallorganisation*. Version 2.1.

Zu diesem Thema könnten Sie auch folgende weitere Umsetzungshilfen interessieren:

- 1.1.5 Kriterien zur Erklärbarkeit der 4.0-Technologien
- 1.2.1 Führung und 4.0-Prozesse
- 1.4.2 Kompetenzen im Führungsprozess 4.0
- 1.4.3 Kompetenzen der Beschäftigten in 4.0-Prozessen
- 1.5.1 Unternehmenskultur in 4.0-Prozessen
- 2.1.2 Integration von intelligenter Software (inkl. KI) in die Organisation
- 2.2.1 Risikobetrachtung von 4.0-Prozessen
- 2.2.2 Gefährdungsbeurteilung 4.0
- 2.2.3 Risikobetrachtung und IT-Sicherheit
- 2.3.1 Datensicherheit in 4.0-Prozessen
- 2.3.2 Datenschutz in 4.0-Prozessen
- 2.4.1 Prozessplanung mit CPS
- 2.5.1 Anforderungen an eine Cloud
- 2.5.3 Plattformökonomie
- 3.2.4 Exoskelette
- 3.2.6 Augmented Reality – Virtual Reality (künstliche Welten)
- 3.2.7 Nutzung von Robotern

Herausgeber: „Offensive Mittelstand – Gut für Deutschland“ – Stiftung „Mittelstand – Gesellschaft – Verantwortung“
Kurfürsten-Anlage 62, 69115 Heidelberg, E-Mail: info@offensive-mittelstand.de; Heidelberg 2019